# *Consequence-Driven Cybersecurity for High-Power EV Charging Infrastructure*

**PI: Barney Carlson**
Idaho National Laboratory

June 4, 2020

DOE Vehicle Technologies Program Annual Merit Review
INL/MIS-20-57906

**Project ID: ELT199**

*This presentation does not contain any proprietary, or otherwise restricted information*

# Overview:

## Timeline

- Start Date: Oct. 2018
- End Date: Sept. 2021
- 50% complete
  (on schedule)

## Barriers

- Increasing risks from cybersecurity vulnerabilities of EV charging infrastructure with:
  - Higher charge power
  - Increased system complexity
    - Multiple communication protocols
    - Advanced control systems for operational performance, energy management, autonomous operation, and public safety

## Budget

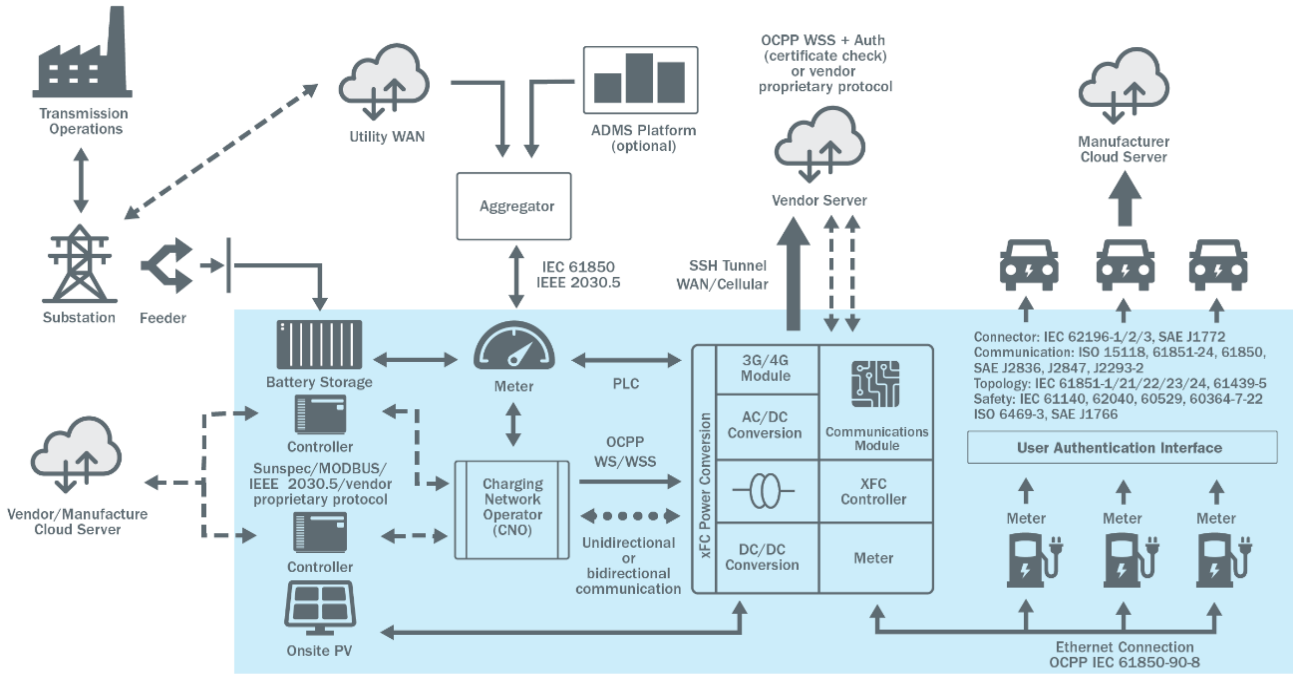
- Total project funding
  - FY20
    - Total: $985k

## Partners

- Project lead
  - Idaho National Lab (INL)
- National lab collaboration
  - National Renewable Energy Lab (NREL)
  - Oak Ridge National Lab (ORNL)
- Industry collaboration
  - ABB
  - Tritium
  - Electrify America

# Relevance:

- Reduce risks associated with potential vulnerabilities for high power EV charging infrastructure leading to high consequence events (HCE)
  1. Safety
  2. Impact to the electric grid
  3. Hardware damage
  4. Denial of service
  5. Data theft or alteration
- With enough time & effort, nearly any electrically controlled system can be accessed or compromised

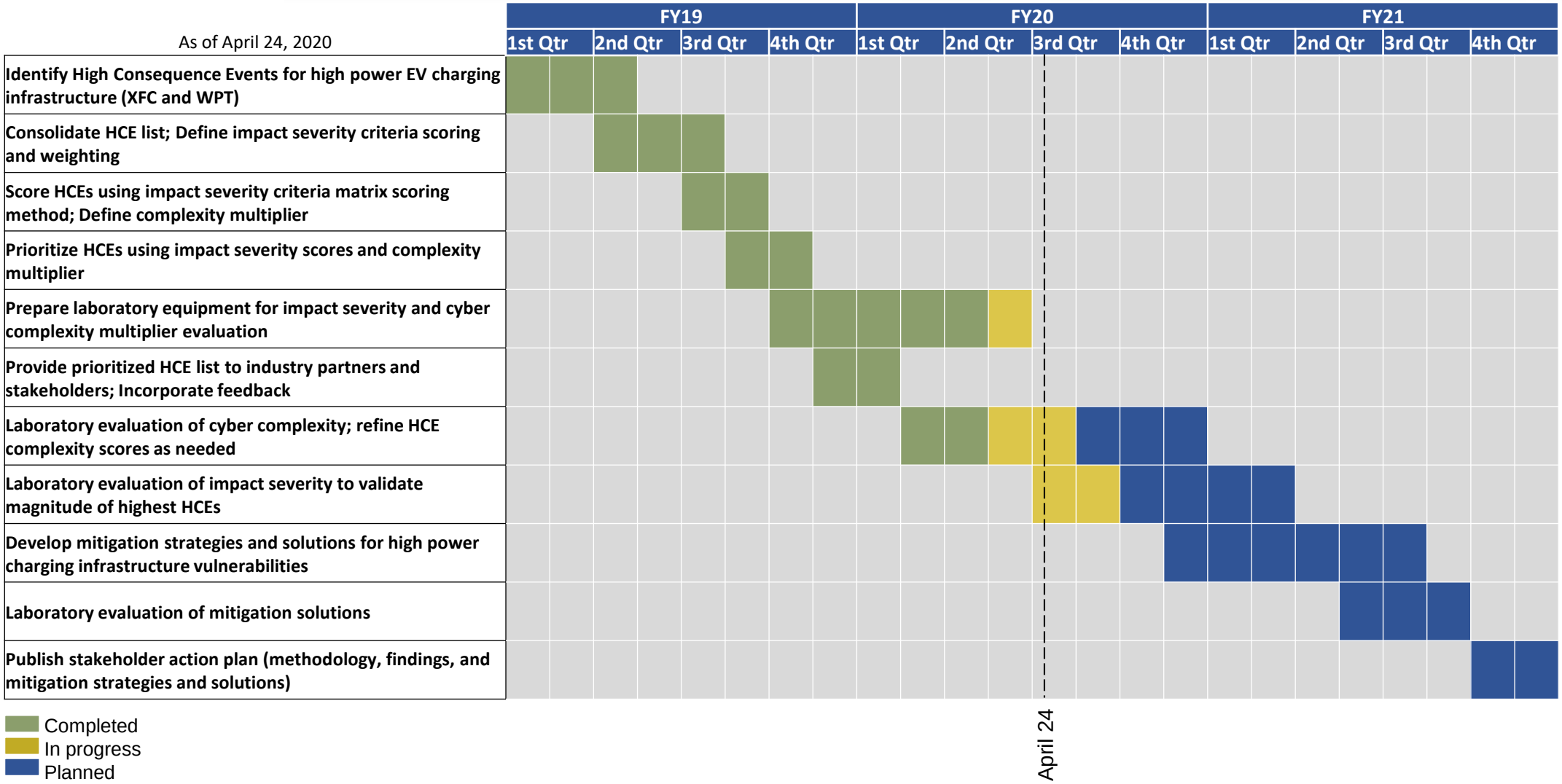



source: NREL

# Objective:

- Determine high consequence events (HCE)
- Prioritize HCEs to guide future research efforts
  - Based on impact severity & cybersecurity manipulation complexity
- Develop mitigation strategies and solutions
- Publish solutions, information, and lessons learned

# Milestones / Timing:




*Any proposed future work is subject to change based on funding levels*

# Approach:

- Conceptualize high consequence events (HCE)

- Prioritize HCEs
  - Based upon **Impact Severity** & cyber manipulation **Complexity Multiplier**
    - Scoring system is similar to DFMEA methodology

- Laboratory evaluation of HCEs:
    - Cybersecurity manipulation complexity
      - Cybersecurity assessment of hardware controls and communications
    - Impact severity
      - Laboratory testing and evaluation to quantify potential impacts
  - Refine HCE prioritization scoring based on laboratory evaluation

- Develop mitigation solutions and strategies
  - Evaluate solutions in laboratory

- Publish results, findings, and mitigation solutions & strategies

# Approach: HCE Ranking Prioritization

HCE Score = Impact x Complexity

- Impact Severity score
  - Severity based on 8 criteria
  - Weighting factor used for the 8 criteria
- Complexity Multiplier score
  (ease of cyber-manipulation)
  - Validate complexity score with laboratory vulnerability assessments
- Scoring similar to DFMEA methodology

## HCE Scoring

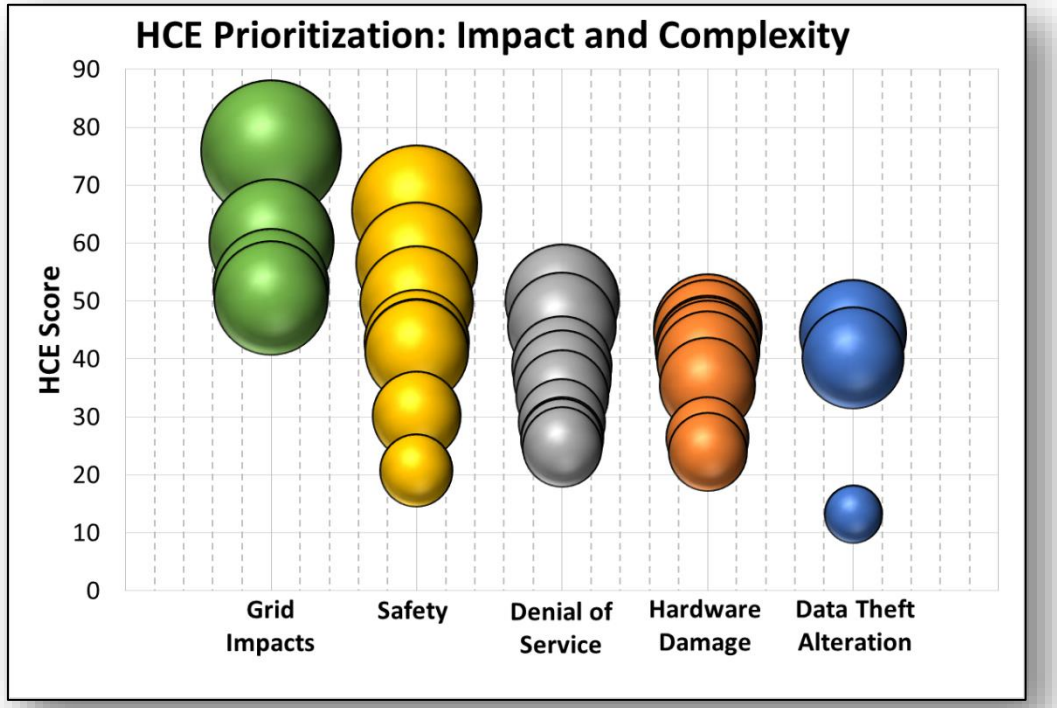
| Complexity Multiplier | Impact Severity | | | | |
|---|---|---|---|---|---|
| **10** | 20 | 40 | 60 | 80 | 100 |
| **8** | 16 | 32 | 48 | 64 | 80 |
| **6** | 12 | 24 | 36 | 48 | 60 |
| **4** | 8 | 16 | 24 | 32 | 40 |
| **2** | 4 | 8 | 12 | 16 | 20 |
| **0** | **2** | **4** | **6** | **8** | **10** |

## Impact Severity Scoring

| Criteria | N/A (0) | Low (2) | Medium (6) | High (10) |
|---|---|---|---|---|
| **Level of Impact** | N/A | Single unit affected (EV, XFC, or WPT) | Multiple units at a single site affected (EV, XFC and/or WPT) | Multiple unit at multiple sites affected (EV, XFC and/or WPT) |
| **Magnitude (proprietary or standardized)** | N/A | Manufacturer specific protocol implementation (EV or EVSE) | >1 manufacturers protocol implementation (supply chain) (EV or EVSE) | Across all standardized systems (both EVSE and EVs) |
| **Duration** | N/A | < 8 hours | > 8hr to < 5 days | > 5 days |
| **Recovery Effort** | Automated recovery without external intervention | Equipment can be returned to operating condition via reset or reboot (performed remotely or by on-site personnel) | Equipment can be returned to normal operating condition via reboot or servicing by off-site personnel (replace consumable part; travel to site) | Equipment can be returned to normal operating condition only via hardware replacement (replace components, requires special equipment, replace entire units) |
| **Safety** | No risk of injury | Risk of Minor injury (no hospitalization), NO risk of death | Risk of serious injury (hospitalization), but low risk of death | Significant risk of death |
| **Costs** | No Cost incurred | Cost of the event is significant, but well within the organization's ability to absorb | Cost of the event will require multiple years for financial (balance sheet) recovery | Cost of the event triggers a liquidity crisis that could result in bankruptcy of the organization |
| **Effect Propagation Beyond EV or EVSE** | No propagation | Localized to site | Within metro area; within single distribution feeder | Regional; impact to several distribution feeders |
| **EV Industry Confidence, Reputation Damage** | No impact to confidence or reputation | Minimal impact to EV adoption | Stagnant EV adoption | Negative EV adoption |

# Accomplishments: Prioritized HCE List

- Prioritized HCEs based on impact severity and cyber manipulation complexity:
  1. *Grid Impacts*: Utility power disruption due to sudden load shed or increase of XFC site
     - XFCs concurrently stop charging (load shed) or site ESS step load increase
  2. *Safety:* Shock / burn hazard from damaged cord set due to thermal cooling system manipulation
  3. *Safety:* EM-field public exposure near wireless charger
     - Especially people w/ a portable medical devices (pacemakers, insulin pumps, etc.)
  4. *Grid Impacts*: Charger site non-responsive to load management or aggregator commands
     - Curtailment requests, VAR support, load scheduling
  5. *Grid Impacts*: Feeder equipment damage
     - Overload, extended operation outside of nominal conditions, cycling resulting in reduced hardware life
  6. *Loss of Service*: No power transfer functionality
     - Error state in charger or site controls caused by cyber manipulation
  7. Approx. 45 more…….



# Accomplishment: Cybersecurity Assessment: ABB TerraHP (XFC)

1. **Identify Attack Pathways**
   - Cellular access via ABB network, local connection, and physical access (open the enclosure)

2. **Identify Vulnerabilities**
   - No “high” or “critical” known vulnerabilities in OpenSSH version 7.5
   - OCPP “man-in-the-middle” attack techniques
   - Physical access has greatest risks

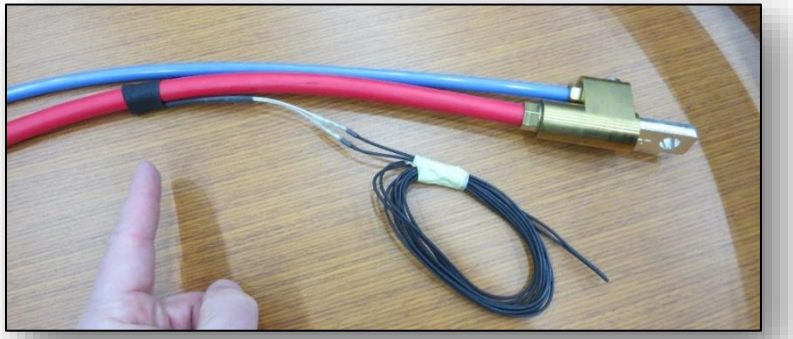
3. **Attempt System Compromise**
   - Potential for remote compromise: very low w/ OpenSSH
   - OCPP1.6 client evaluation and pen testing is under way
   - Unauthorized access is likely only with physical access
     - But protections are very strong
       - Access attempts failed via: USB, bootloader, MicroSD, keyboard, etc.

4. **Provide Mitigation Recommendations**
   - Mitigation solutions will be developed, evaluated, and published in later stages of this project (year 3)

# Accomplishments: Cyber Complexity Eval. of highly scored HCE

- XFC cable liquid cooling system manipulation
  - Thermal sensors spoofing may cause lack of thermal control
    - Burn hazard
    - Possible insulation failure
  - Unique vulnerability to XFC

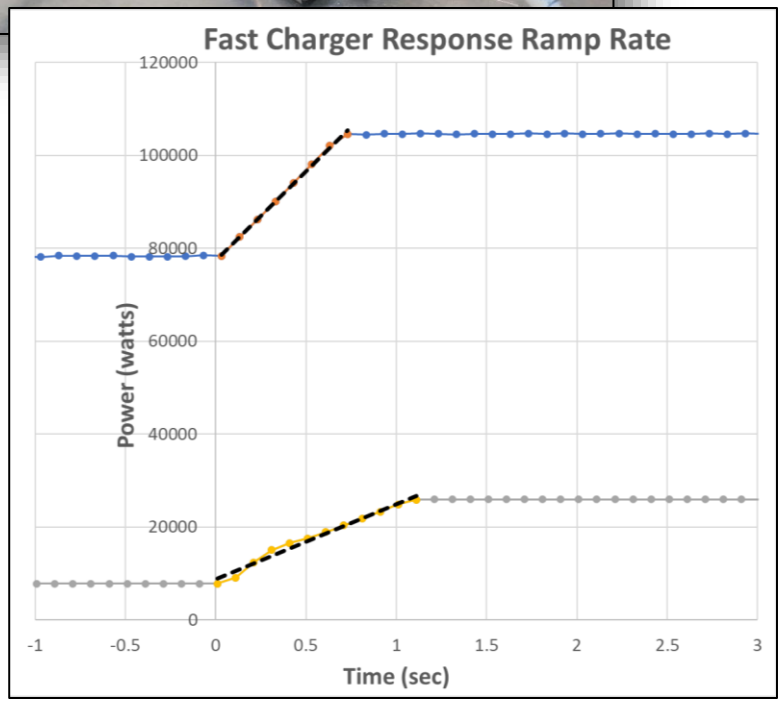
- Cyber Complexity Evaluation Results:
  - Cable temperature sensors are analog thermistors
    - Difficult to spoof
  - Industry standards: also include vehicle inlet coupler temperature measurement
    - ISO 17409
    - IEC 61851-23 ed.2
  - Increased cyber complexity: vehicle inlet port and the CCS cable temperature measurements must both be spoofed
    - Very difficult
- Conclusion:
  - Significantly reduced HCE score due to increased cyber complexity



# Accomplishments: Cyber Complexity Evaluation

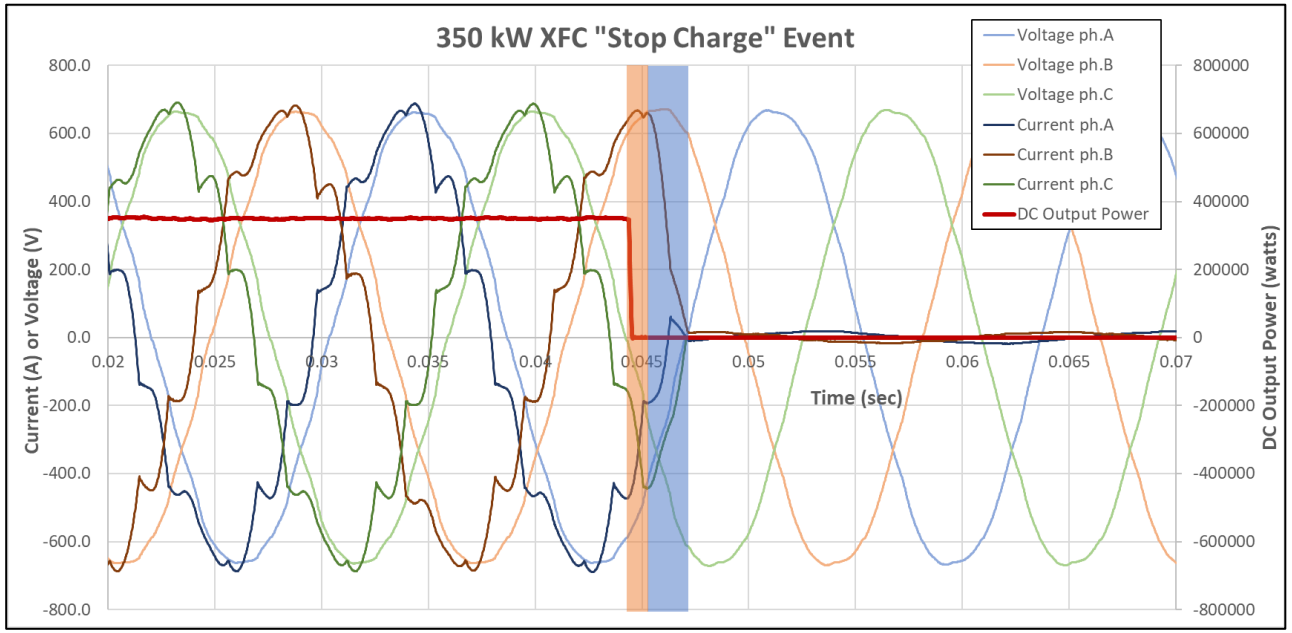
- OCPP 1.6 (JSON) local server (SteVe) at INL
  - Running on a Raspberry PI
  - Communication with:
    - XFC (350kW)
    - DCFC (50kW)

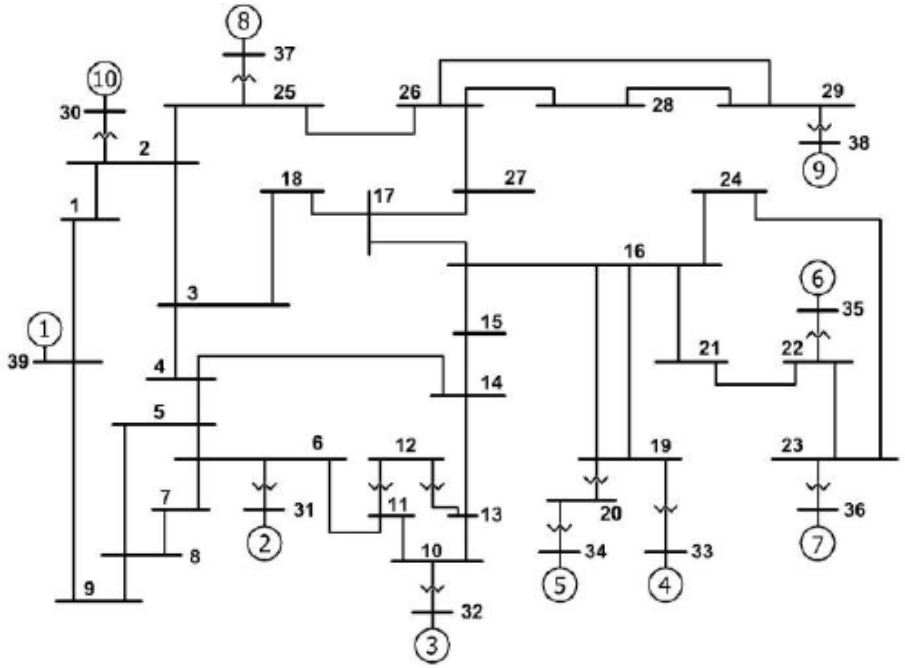
  - Primary Concern:
    - Coordinated energy management manipulation
      - Potential for significant load mis-management
        - Increased load during curtailment request
      - Denial of service for energy management control
        - Non-responsive to requests
  - Minor concern:
    - Stability impact from power fluctuation manipulation
      - Ramp rate:15kW/sec to 40kW/sec
        - Very slow in comparison to load shed



# Accomplishments: Impact Severity Evaluation

- Grid Impacts from simultaneous load shed from multiple XFC
  - Shut down response of one XFC
    - 2.0 to 3.0 msec. (-175 MW/sec) from full power (350kW) to standby power
  - RSCAD modeling of load shed event using model of 39 bus system is in progress
    - Simulation sensitivity parameters
      - XFC loading (quantity, proximity, power level)
      - Distribution feeder loading
      - XFC ramp rate sensitivity



# Future Research: Continue Validation & Mitigation Development

- Assess the *highest* prioritized HCEs:
  - Validation of cyber manipulation complexity:
    - Laboratory hardware evaluation
  - Evaluation of impact severity:
    - Potential impact to the grid
    - Charger hardware manipulation in laboratory
  - Develop strategies and solutions for prioritized HCEs
    - Solutions to hardened attack surfaces of vulnerabilities
    - Methodology to safeguard personal information & data
    - Methods to identify occurrence of cyber malicious event
    - Develop response mitigation strategies and solutions
- Publish findings and lessons learned
  - Prioritized list of HCEs
  - Results from laboratory evaluations
    - Impact Severity
    - Cyber manipulation complexity
  - Mitigation solutions & strategies

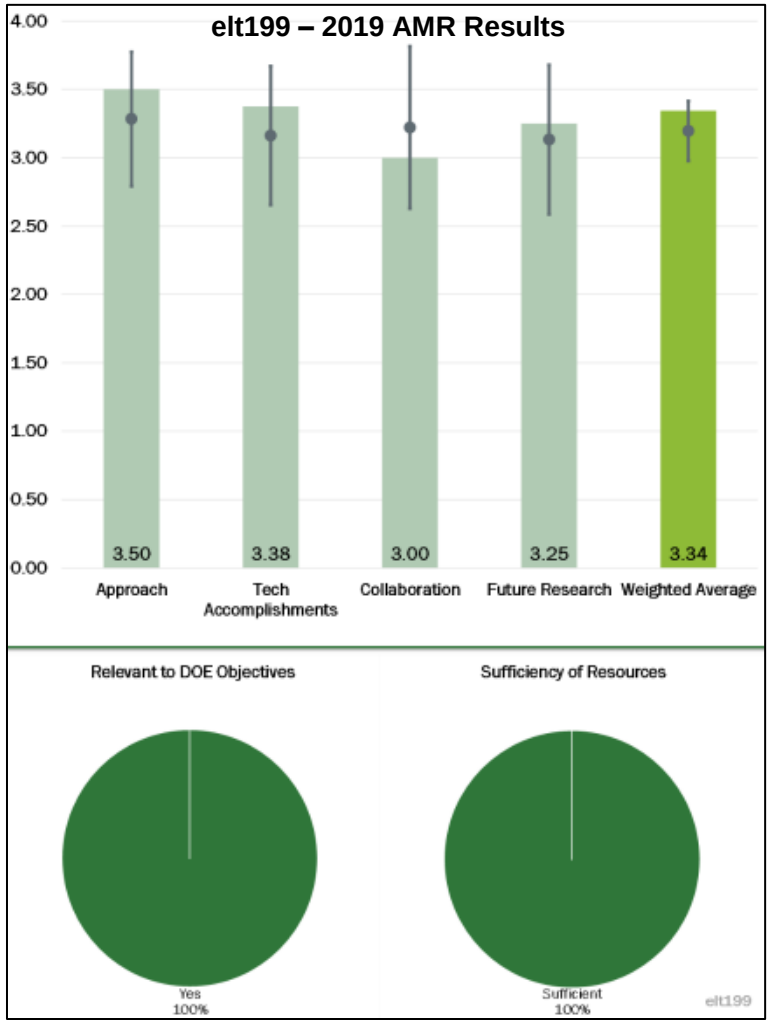

*Any proposed future work is subject to change based on funding levels*

# Response to Previous Year Reviewer Comments and Questions

- *Reviewer comment*: "The proposed work on developing mitigation strategies and solutions is particularly important."
  - *Response*: Development of mitigation solutions & strategies is planned to begin in the 4th Qtr of the 2nd year (FY20).

- *Reviewer question*: "…project team talks about providing solutions to their partners, how they account for other utilities or infrastructure industries that may need the information?"
  - *Response*: In fY21, the team will publish results, findings, lessons learned, and mitigation solution and strategies. These outputs will also be conveyed to industry working groups as security solutions and recommendations.

- *Reviewer question*: "…how the team will provide lessons learned to other stakeholders that are not part of the team?"
  - *Response*: In fY21, the team will publish results, findings, lessons learned, and mitigation solution and strategies. These outputs will also be conveyed to industry working groups as security solutions and recommendations.



# Collaboration

- Team collaboration includes:
  - National labs
    - INL, NREL, ORNL
  - Charger equipment manufacturers
    - Tritium, ABB
  - Charge Site owner / operator
    - Electrify America

- Additional EV charging infrastructure cybersecurity collaboration:
  - VOLPE / NMFTA: MD/HD truck high power charging infrastructure
    - cybersecurity guidelines and recommended best practices
  - 21st Century Truck Electrification Tech Team: Charging & Infrastructure Working group
    - cybersecurity requirements and guidelines
  - WAVE Inc.: MD/HD wireless charging at 250+ kW
  - Utah State Univ.: static & dynamic WPT control strategies strategy development
  - Four other US DOE funded, EV charging infrastructure cybersecurity projects
    - Sandia National Lab, Virginia Tech, EPRI, ABB “CyberX”

# Summary:

- Conceptualize high consequence events (HCE) for high power EV charging infrastructure

- Prioritize HCEs
  - Based upon **Impact Severity** & cyber manipulation **Complexity Multiplier (**similar to DFMEA)

- Laboratory evaluation of HCEs:
    - Cybersecurity manipulation complexity
      - Hardware controls and communication systems evaluation
    - Impact severity
      - Laboratory testing
  - Refine HCE prioritization scoring based on laboratory evaluation

- Develop mitigation solutions and strategies
  - Evaluate solutions in laboratory

- Publish results, findings, and mitigation solutions & strategies